
VeriSign Trust Network Certificate Policies

Certificate Interoperability Service (CIS) CP Supplement



Version 1.4

May 31, 2006



VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
+1 650.961.7500
<http://www.verisign.com>

VeriSign Trust Network Certificate Policies

© 2004 VeriSign, Inc. All rights reserved.
Printed in the United States of America.

Revision date: August 5, 2004

Trademark Notices

VeriSign and the name of VeriSign products described in this document are registered trademarks of VeriSign, Inc. The VeriSign logo and VeriSign Trust Network are trademarks and service marks of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of VeriSign, Inc.

Notwithstanding the above, permission is granted to reproduce and distribute these VeriSign Certificate Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to VeriSign, Inc.

Requests for any other permission to reproduce these VeriSign Certificate Policies (as well as requests for copies from VeriSign) must be addressed to VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.961.7500 Fax: +1 650.426.7300 Net: **practices@verisign.com**.

VTN CIS CP Supplement

History of changes: version 3.2 (Effective date May 01, 2006)

Section Number	Description of change
6.3.2 (Table 9)	Added: 1. VeriSign to CIS Customer offline CA with a maximum validity of 10 years 2. Updated validity period of issuing CAs to 7 years 3. Provided that encryption only End-User Subscriber certificates may be issued for 3 years
Section 7.1.2.4	Clarified that CA Certificates issued to CIS Customers' for issuing End-User certificates shall have a set the "PathLenConstraint" field set to a value of "0".

TABLE OF CONTENTS

1. Introduction	1
1.1 Overview.....	2
1.1.1 Policy Overview.....	6
1.2 Identification.....	8
1.3 Community and Applicability.....	8
1.3.4 Applicability	8
1.3.4.1 Suitable Applications	8
1.3.4.1.4 CIS Type 1-2 Certificates	8
1.4 Contact Details	8
1.4.3 Person Determining CPS Suitability for the Policy	8
2. General Provisions	9
2.1 Obligations (Type 1-2)	9
2.1.5 Repository Obligations	9
2.2 Liability (Type 1-2)	9
2.2.1.3 Certification Authority Limitations of Liability.....	9
2.2.3 Subscriber Liability	9
2.2.3.1 Subscriber Warranties	9
2.5 Fees (Type 1-2)	9
2.7 Compliance Audit.....	10
2.7.1 Frequency of Entity Compliance Audit (Type 1-2).....	10
2.7.2 Identity/ Qualifications of Auditor.....	10
2.7.4 Topics Covered by Audit	10
2.7.4.5 Audit of CIS Customer (Type 1-2)	10
3. Identification and Authentication	10
3.1 Initial Registration	10
3.1.1 Types of Names (Type 1-2).....	10
3.1.4 Uniqueness of Names (Type 1-2)	10
3.1.8 Authentication of Organization Identity.....	10
3.1.9 Authentication of Individual Identity.....	11
3.1.9.2 Class 2 and Type 2 Certificates.....	11
3.1.9.2.1 Class 2 Managed PKI Certificates and Type 2 CIS Certificates.....	11
4. Operational Requirements	11
4.1 Certificate Application (Type 1-2).....	11
4.1.1 Certificate Applications for End-User Subscriber Certificates.....	11
4.4 Certificate Suspension and Revocation (Type 1-2).....	11
4.4.9 CRL Issuance Frequency (If Applicable)	11
4.4.15 Special Requirements Regarding Key Compromise	12
4.5 Security Audit Procedures	12
4.5.1 Types of Events Recorded	12
4.5.1.4 Events Recorded by CIS Customers (Type 1-2).....	12
4.8 Compromise and Disaster Recovery (Type 1-2).....	13
5. Physical, Procedural, and Personnel Security Controls	13

5.1 Physical Controls	13
5.1.1 Site Location and Construction	13
5.1.1.5 CIS Customer Requirements (Type 1-2)	13
5.1.2 Physical Access	13
5.1.2.4 Requirements for CIS Customers (Type 1-2)	13
5.2 Procedural Controls	14
5.2.1 Trusted Roles	14
5.2.1.1 CIS Customer (Type 1-2)	14
5.2.2 Number of Persons Required Per Task (Type 1-2)	14
6. Technical Security Controls	14
6.1 Key Pair Generation and Installation	14
6.1.1 Key Pair Generation (Type 1-2)	14
6.1.2 Private Key Delivery to Entity (Type 1-2)	15
6.1.9 Key Usage Purposes (As per X.509 v3 Key Usage Field) (Type 1-2)	15
6.2 Private Key Protection	16
6.2.1 Standards for Cryptographic Modules (Type 1-2)	16
6.2.3 Private Key Escrow (Type 1-2)	16
6.2.4 Private Key Backup (Type 1-2)	16
6.2.7 Method of Activating Private Key	16
6.2.8 Method of Deactivating Private Key	16
6.3.2 Usage Periods for the Public and Private Keys	17
6.4 Activation Data	17
6.4.1 Activation Data Generation and Installation	17
6.4.1.4 Processing Centers and CIS Customers (Type 1-2)	17
6.4.2 Activation Data Protection	17
6.5 Computer Security Controls	18
6.5.1 Specific Computer Security Technical Requirements	18
6.5.1.4 Controls for CIS Customers (Type 1-2)	18
6.5.2 Computer Security Rating (Type 1-2)	18
6.6 Life Cycle Technical Controls (Type 1-2)	18
6.6.1 System Development Controls	18
6.6.1.3 CIS Customers (Type 2)	18
6.6.2 Security Management Controls	19
6.6.2.3 Software Used by CIS Customers (Type 2)	19
7. Certificate and CRL Profile	19
7.1 Certificate Profile	19
7.1.2.4 Basic Constraints	19
7.1.6 Certificate Policy Object Identifier	19
8. Specification Administration (Type 1-2)	20
8.3 CPS Approval Procedures	20
9. Appendix	20
9.1 Acronyms and Definitions	20
9.2 Section Number Cross Reference	21

1. Introduction

This document is a supplement to the *VTN Certificate Policy* (“VTN CP”) whose object identifiers are 2.16.840.1.113733.1.7.23.1 and 2.16.840.1.113733.1.7.23.2. It describes the minimum certificate policies required for participation in the VeriSign Certificate Interoperability Service (CIS) offering. Given the fact that this is a VTN CP supplement, only the sections that further define CIS’s implementation will be documented herein. CIS Customers are required to adhere to this CP Supplement as well as the VTN CP. This CP Supplement supercedes any conflicting language found in the VTN CP. Section headings in this document containing no specifics are presented for clarity and context; the actual language is contained within the VTN CP.

Please Note: The capitalized terms in this CP are defined terms with specific meanings. Please see Section 9 for a list of definitions.

Several VTN CP sections only required “CIS Customer” text to be inserted. These sections have been omitted from this supplement to keep the size of this document relatively small; therefore, where not specifically noted, CIS Customers shall follow the VTN CP requirements in different designated roles (please note that some sections require multiple roles). This is due to the unique nature of a CIS Customer within the VTN which performs similar functions within its Subdomain of operation. **Adherence to specific VeriSign confidential and ancillary documents referenced in the VTN CP is not required for CIS Customers functioning in these roles unless otherwise specified in other agreements.** The roles and associated sections are:

- As a “Processing Center” in VTN CP §§ 2.1.2, 2.6.1, 4.4.3.2, 4.7, 5.2.1.1, 6.2.6, 6.2.9.2, 6.4.3.2, 8.3;
- As an “Affiliate” in VTN CP §§ 2.1.1, 2.2.1, 2.2.2, 2.6.1, 2.6.3, 2.7, 2.8, 2.8.1, 2.8.4, 2.8.5, 2.8.6, 3.1.9, 4.4.1.1, 4.4.10, 4.4.15, 6.1.4, 6.4.1.1;
- As a “Managed PKI Customer” in VTN CP §§ 3.1.8.2, 3.1.9.2, 3.1.9.2.1, 4.1.2, 4.4.1.1, 6.1.3, 6.1.4, 6.1.8;
- As a “Gateway Customer” in VTN CP §§ 2.1.1, 2.2.1, 2.3.3, 3.1.9.1, 3.2.2, 3.4, 4.1.1, 4.2.1, 4.3, 4.4.1.1, 4.4.1.2, 4.4.3.1, 4.5.2, 4.8.3, 4.8.4, 4.9, 5, 5.1.1, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.2.2, 5.2.3, 5.3.2.1, 6.1.8, 6.1.9, 6.2, 6.2.4, 6.6.2.1, 6.7, 7.1 (including all subsections), 7.2; and
- As a “Server Service Center” in VTN CP § 2.1.2.

Where not specifically noted, CIS Type 1 requirements will equate to VTN Class 1 requirements; CIS Type 2 requirements will equate to Class 2 requirements. VeriSign operates its Type 1 and Type 2 signing CAs as Class 1 and Class 2 signing CAs respectively.

VTN CP References to Managed PKI Customers utilizing Managed PKI Key Manager shall be interpreted as CIS Customers utilizing a key escrow system similar to Managed PKI Key Manager.

VTN CP References to Managed PKI Control Center shall be interpreted as CIS Customers utilizing a manual administration tool.

The audience for this document is the governing body of the CIS Customer CA that will be chained to one or more of the VeriSign CIS CAs. Such governing body will provide guidance for the CIS Customer CA's implementation to ensure that compliance assessments can be performed of the CIS Customer's PKI operations to determine suitability for participation in the VeriSign Certificate Interoperability Service offering.

The authors of this document comprise the members of the VeriSign Trust Network Policy Management Authority ("PMA"). The PMA is responsible for proposing changes to the VTN CP, updating the documentation, and soliciting comments on the CP modifications. The PMA also oversees compliance with the requirements of the CP and applicable supplements.

1.1 Overview

The VTN CP establishes requirements for the entire VTN. The VTN CP governs the use of the VTN by all individuals and entities within the VTN (collectively, "VTN Participants"). VeriSign and its CIS Customers worldwide must follow the requirements of the VTN CP. VeriSign and each CIS Customer have authority over a portion of the VTN. The portion of the VTN controlled by VeriSign or a CIS Customer is called its "Subdomain" of the VTN. A CIS Customer's Subdomain consists of its organizational Subscribers. Nonetheless, the CP acts as an umbrella document establishing baseline VTN Standards for the entire VTN.

This CIS CP supplement shall govern all VeriSign CIS CAs, CIS Customer CAs, their RAs, Subscribers, and Relying Parties who participate in the VeriSign Certificate Interoperability Service. This document shall supercede any other CP CIS Supplements that may be referenced in related Certificates or any related agreements.

The VeriSign Certificate Interoperability Service's goal is to provide the capability for privately operated CAs to interoperate with other CAs that are members of the VTN for the purpose of exchanging encrypted and/or digitally signed S/MIME (email) messages. The service simplifies interoperability by allowing CAs to become part of the VTN (VeriSign's public hierarchy) – instead of requiring the private CA to cross certify with every CA that it wishes to interoperate with. The CIS offering and pricing is targeted to a Customer Subdomain having only one CA that issues one Type of Subscriber certificates (no Subordinate Intermediate CAs are allowed). Additional Customer Subdomain CAs may be negotiated and included in the agreement.

The CIS offering provides for two new certificates (Type 1 and Type 2) for the purpose of providing interoperability of S/MIME email message encryption and digital signatures between private CAs (and its end entities) and the VTN public CA (and its end entities).

Type 1 and Type 2 certificates are similar in nature to VTN Class 1 and Class 2 certificates, but are limited to S/MIME encryption and S/MIME digital signature use. The

CIS Customer CA operational requirements are less rigorous than the operational requirements for CAs issuing Class 3 certificates in order to accommodate the constraints of conventional IT environments.

Type 1 and Type 2 policies apply to CIS Customers whose certificates have not been minted by VeriSign under its Class 1 and Class 2 policies. The new policy identifiers will aid relying parties in distinguishing between Type 1-2 and Class 1-2 certificates and policy requirements.

VeriSign accomplishes interoperability by signing a private CA's root certificate such that it chains up to a VeriSign VTN public root CA. During the signing, VeriSign inserts additional information into the CIS Customer's CA certificate to make it compliant with the VTN (See CP § 7.1 for details). VeriSign VTN public root CA certificates are embedded in most web browser and S/MIME software. Once a part of the VTN hierarchy, encrypted and/or digitally signed S/MIME messages will be able to interoperate with other S/MIME implementations that:

- Can resolve to a VeriSign VTN public root certificate;
- Provide a mechanism for their subscribers to locate the certificates of their message recipients (enables encryption);
- Provide a mechanism to allow relying parties to locate the certificates of the message sender (enables digital signature verification); and
- Provide a mechanism for relying parties to check the status of certificates.

Figure 1 provides an illustration of how a typical Type 2 CIS implementation chains to a VeriSign VTN public root CA.

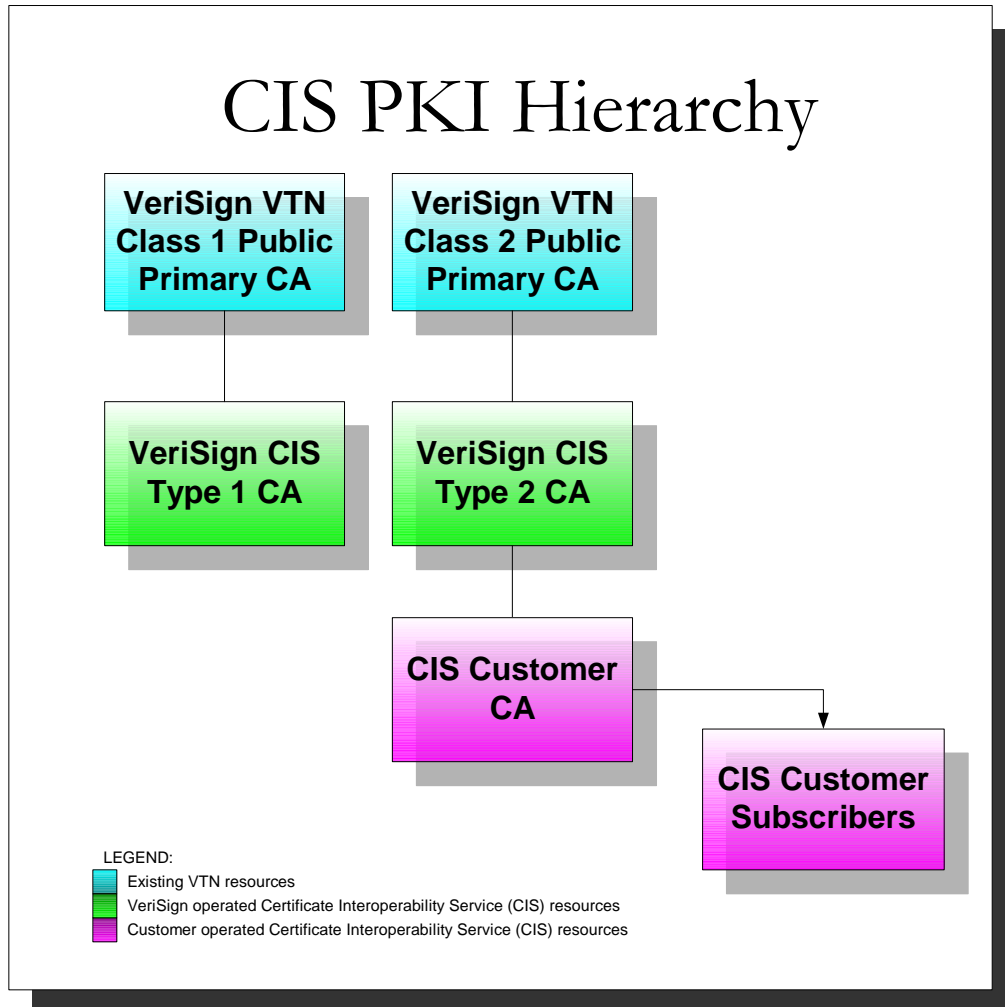


Figure 1. Typical CIS Type 2 Implementation

(a) Role of the VTN CP and Other Practices Documents

There are several documents that make the VeriSign Certificate Interoperability Service possible. In general, a CP governs a Public Key Infrastructure (PKI) implementation by establishing requirements and standards for an implementation. A Certification Practice Statement (CPS) describes how a particular CA has been implemented and how it meets the requirements of the CP. A Subscriber Agreement (SA) defines the legal obligations that a CA makes to its subscribers and their legal obligations to the CA. A Relying Party Agreement (RPA) defines the legal obligations between relying parties and a CA. Figure 2 illustrates the relationship between these documents. (Types of certificates are discussed in CP § 1.1.)

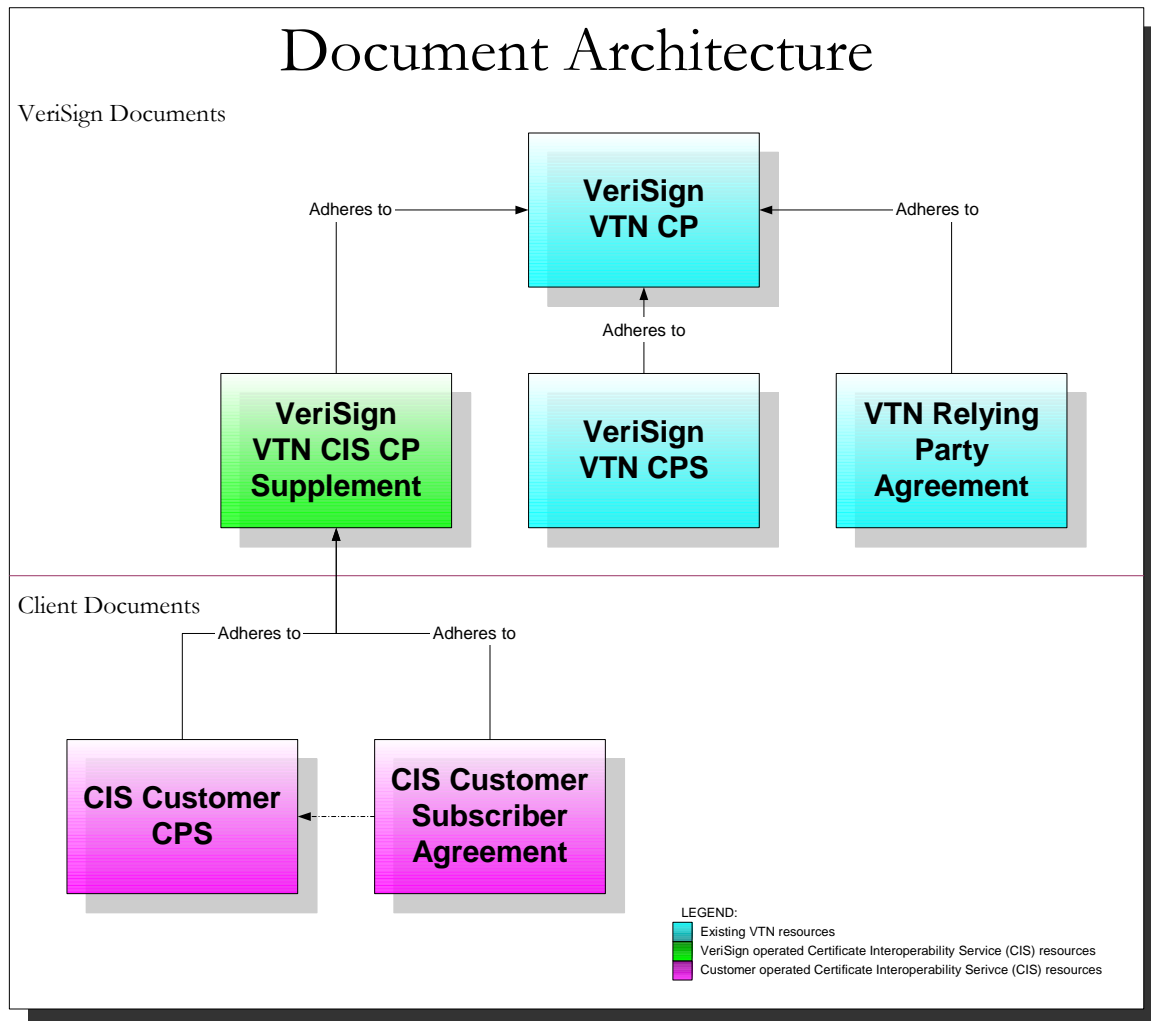


Figure 2. CIS Document Architecture

The **VeriSign VTN CIS CP Supplement** (*this document*) documents the fact that the CIS Type 1 and Type 2 CAs located at VeriSign facilities shall be operated in a manner similar to VeriSign VTN Class 1 and Class 2 CAs. It also governs a customer's PKI implementation by establishing the minimal set of requirements for participation in the VeriSign Certificate Interoperability Service. It will be used as a controlling input to the CIS compliance assessment process. This document may be integrated into the VTN CP and VTN CPS documents in a future release.

CIS Customer CPS describes how CIS Customer's PKI implementation meets the *VeriSign CIS VTN CP Supplement* requirements. CIS Customers use VeriSign's CIS CPS template which is a quick-start document provided by VeriSign to its CIS customers in instances when the customer complies with all the provisions. The template is appropriately modified to reflect the Customer's environment during the initial CIS implementation. VeriSign, in the CIS Agreement, grants a perpetual license for the CIS Customer to use the VeriSign CIS CPS language as long as the CIS Agreement is in effect. VeriSign retains all intellectual property rights to the CIS Customer CPS.

CIS Customer Subscriber Agreement specifies customer subscriber obligations for CIS participation. This is a quick-start document provided by VeriSign to its CIS customers. It shall adhere to the VTN CP and CIS CP Supplement; it may optionally be required by the CIS Customer's CPS.

All CIS relying parties shall adhere to the requirements of the **VeriSign VTN Relying Party Agreement**.

CIS Customers are required to follow the VTN CP and CIS CP Supplement, maintain their own CPS, maintain their own Subscriber Agreement, and utilize the VTN Relying Party Agreement.

Table 1 is a matrix showing various VTN practices documents as they apply to CIS Customers. The list in Table 1 is not intended to be exhaustive. Note that documents not expressly made public are confidential to preserve the security of the VTN.

Documents	Status	Where Available to the Public
VeriSign Trust Network Certificate Policies	Public	VeriSign Repository per CP § 8.2.2. See https://www.verisign.com/repository
VeriSign- or CIS Customer-Specific Documents		
VeriSign Certification Practice Statement	Public	VeriSign Repository per CP § 2.6.1. See https://www.verisign.com/repository
CIS Customers' CPSs	Public	CIS Customers' repositories per CP § 2.6.1. See repository sections of CIS Customers' web sites. (CIS Customers may elect by contractual agreement to have VeriSign publish their CPSs in the VeriSign repository.)
VeriSign's ancillary agreements (Managed PKI Agreements, Subscriber Agreements, and Relying Party Agreements)	Public, including Managed PKI Lite agreements, but not Managed PKI agreements, which are confidential	VeriSign Repository per CP § 2.6.1. See https://www.verisign.com/repository
CIS Customers' ancillary agreements	Form web-based agreements are public, but agreements with enterprise Customers are not.	CIS Customers' repositories per CP § 2.6.1. See repository sections of CIS Customers' web sites.

Table 1 – Availability of Practices Documents

1.1.1 Policy Overview

VeriSign's Certificate Interoperability Service (CIS) offers two additional types of S/MIME Certificates that are generated by CIS Customer CAs: Type 1 and Type 2. The

service provides a mechanism for S/MIME interoperability for CAs that are not operated or hosted by VeriSign or an Affiliate.

Type 1 Certificates, issued only to individuals, provide the lowest level of assurances within the VTN. They provide assurances that the Subscriber's distinguished name is unique and unambiguous within a CIS Customer's Subdomain and that a certain e-mail address is associated with a public key. They are limited to S/MIME digital signatures and encryption use where proof of identity is unnecessary.

Type 2 Certificates, also issued only to individuals, provide a medium level of assurances within the VTN. They provide assurances of the identity of the Subscriber based on a comparison of information submitted by the Certificate applicant against information in CIS Customer business records or databases. They are limited to S/MIME digital signatures and encryption use where proof of identity is required.

Table 2 sets forth the properties of each CIS Certificate Type issued by CIS Customers.

Class	Issued to	Services Under Which Certificates are Available	Confirmation of Certificate Applicants' Identity (CP §§ 3.1.8.1, 3.1.9)	Applications implemented or contemplated by Users (CP § 1.3.4.1)
Type 1	Individuals	CIS	Name and e-mail address search to ensure uniqueness plus checking of internal documentation or databases to confirm the Certificate Applicant is affiliated with the CIS Customer.	Similar to Class 1, but physical security and hosting of CA systems is not performed by VeriSign (some requirements are relaxed). Modestly enhancing the security of e-mail through confidentiality encryption and digital signatures where proof of individual identity is unnecessary.
Type 2	Individuals	CIS	Name and e-mail address search, automated or manual checking of internal documentation or databases to confirm identity of the Certificate Applicant (e.g., human resources documentation) and that the Certificate Applicant is affiliated with the CIS Customer.	Similar to Class 2, but physical security and hosting of CA systems is not performed by VeriSign (some requirements are relaxed). Enhancing the security of e-mail through confidentiality encryption and digital signatures for individual authentication.

Table 2 - Certificate Properties Affecting Trust

The specifications for CIS Types of Certificates in this CP set forth the minimum level of assurances provided for each Class. Nonetheless, by contract or within specific environments (such as an intra-company environment), VTN Participants are permitted to use validation procedures stronger than the ones set forth within the CP, or use Certificates for higher security applications than the ones described in CP §§ 1.1.1,

1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CP §§ 2.2.1.2, 2.2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.2 Identification

For CIS Customers, the following object identifier values are used in end-user CIS Subscriber Certificates:

- The Type 1 Certificate Policy: VeriSign/pki/policies/cis/type1 (2.16.840.1.113733.1.7.46.1)
- The Type 2 Certificate Policy: VeriSign/pki/policies/cis/type2 (2.16.840.1.113733.1.7.46.2)

1.3 Community and Applicability

1.3.4 Applicability

1.3.4.1 Suitable Applications

1.3.4.1.4 CIS Type 1-2 Certificates

Certificates used for interoperability through the VeriSign Certificate Interoperability Service are limited by Type of Certificate. Specifically, VeriSign Certificate Interoperability Service participation limits the use of certificates to the following categories of operation:

- Type 1 – S/MIME encryption and S/MIME digital signatures (Certificate Subject name is email address)
- Type 2 – encryption and digital signature applications (Certificate Subject name is associated with an individual's identity, as verified per CP § 3.1.9, and associated with an email address belonging to that individual) Email aliases not tied to a specific authenticated individual are not supported under the Type 2 Certificate offering due to digital signature non-repudiation and private key control requirements.

CIS Customer CAs may only issue certificates to human subscribers. Non-human subscribers are expressly forbidden. Use of the certificate must in all cases be under the conscious control of the nominal subscriber, and such control cannot be delegated to a device.

1.4 Contact Details

1.4.3 Person Determining CPS Suitability for the Policy

The persons determining whether the CPS of a CIS Customer is suitable for this CP are members of the VeriSign Policy Management Authority (PMA).

2. General Provisions

2.1 Obligations (Type 1-2)

2.1.5 Repository Obligations

For a CIS Customer, the VeriSign or affiliated Processing Center shall publish the CIS Customer's CA certificate signed by VeriSign.

CIS Customers are responsible for the repository functions of their own subdomain. At a minimum the repository must use an X.500 directory service accessible through LDAP and deploy access control mechanisms as required to secure its data. Information posted must include, but is not limited to: Certificates, Certificate Policies, Certification Practice Statements, any Agreements, and Certificate status information in the form of CRLs or interactive query (if appropriate). The repository shall be publicly accessible by CIS Customer Subscribers and any Relying Parties.

Upon revocation of an end-user Subscriber's Certificate, the CIS Customer that issued the Certificate shall publish notice of such revocation in its repository. In addition, CIS Customers shall issue CRLs for the CAs within their Subdomains, pursuant to CP §§ 4.4.9, 4.4.11.

CIS Customers may elect to contractually allow VeriSign to host CIS Customer repository functions.

2.2 Liability (Type 1-2)

2.2.1.3 Certification Authority Limitations of Liability

VeriSign does not provide liability insurance. CIS Customers may elect to obtain liability insurance independently.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

Subscribers shall warrant that no unauthorized person has ever had access to the copy of the Subscriber's private key on the Subscriber's hardware/software platform. These Subscribers make no warranty concerning the copies of their private keys in the possession of the CIS Customer's key escrow system.

2.5 Fees (Type 1-2)

CIS Customers shall not charge fees to its Subscribers for certificate issuance, renewal, access, revocation, status information, policy documentation or other PKI-related services.

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit (Type 1-2)

Compliance Audits shall be conducted at least annually at the sole expense of the audited entity. Type 1 CIS Customers shall be audited at least once every two (2) years.

2.7.2 Identity/ Qualifications of Auditor

CIS Customers shall be audited by VeriSign or a third party auditor approved by VeriSign.

2.7.4 Topics Covered by Audit

2.7.4.5 Audit of CIS Customer (Type 1-2)

CIS Customers shall be audited pursuant to the published CIS Customer assessment criteria as identified in the CIS Master Services Agreement.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names (Type 1-2)

Additionally, Type 1 Certificates shall contain a valid email address in the Subject distinguished name field or Subject Alternative Name field and shall adhere to RFC 822 specifications for Internet email addresses. If the Subject distinguished name field is null, then the Subject Alternative Name field shall be marked critical.

For all CIS Customer Certificates (i.e., Type 1 Subscriber, Type 2 Subscriber, and CIS Customer CA Certificates): The organization value (O=) in the Subject field shall be set to the legal name of the CIS Customer's organization.

3.1.4 Uniqueness of Names (Type 1-2)

Additionally, Issuing CAs may elect to guarantee continuity uniqueness of certificate names such that a distinguished name for a given entity shall not be used in the future to refer to another entity (e.g., the name *John Smith* shall not be used for a different John Smith. The name may only be re-used if the original John Smith rejoined the community).

3.1.8 Authentication of Organization Identity

3.1.8.2 Authentication of the Identity of CAs and RAs (Type 1-2)

CIS Customers, before becoming CAs or RAs, enter into an agreement with an entity above it within the Type 1, 2 VTN hierarchy (the "Superior Entity"). The table below shows the possible Superior Entities corresponding to each CA Certificate Applicant.

CA or RA	Superior Entity
CIS Customer	VeriSign

Table 6 – CAs and RAs and Their Superior Entities

3.1.9 Authentication of Individual Identity

Additionally, CIS Customers shall approve a Certificate Application only if the Certificate Applicant is an Affiliated Individual to the CIS Customer. If a Subscriber who had been issued a Certificate by the CIS Customer ceases to be affiliated with the CIS Customer as an Affiliated Individual, then the CIS Customer shall promptly request revocation of such Subscriber's Certificate.

3.1.9.2 Class 2 and Type 2 Certificates

3.1.9.2.1 Class 2 Managed PKI Certificates and Type 2 CIS Certificates

Additionally, CIS Customers may develop their own administrator and automated administration tools to approve certificate applications.

3.2 Routine Rekey (Renewal) (Type 1-2)

Rekey/renewal is subject to constraints of CP § 6.3.2.

4. Operational Requirements

4.1 Certificate Application (Type 1-2)

4.1.1 Certificate Applications for End-User Subscriber Certificates

Table 7 additions for CIS Customers are:

Certificate Class	Entity Processing Certificate Applications	Entity Issuing Certificate
CIS CA Certificate	VeriSign or Affiliate Processing Center	VeriSign or Affiliate Processing Center
Type 1 individual Certificate	CIS Customer	CIS Customer
Type 2 individual Certificate	CIS Customer	CIS Customer

Table 7 – Entities Receiving Certificate Applications

4.4 Certificate Suspension and Revocation (Type 1-2)

4.4.9 CRL Issuance Frequency (If Applicable)

VeriSign shall publish revoked CIS CA Certificates of CIS Customers in its repository. CIS Customers are responsible for publishing CRL information of its Subscribers.

The CIS Customer CA shall publish CRLs for such Type 2 certificates within 24 hours of

notification. The CIS Customer CA shall publish CRLs for such Type 1 certificates within 7 days of notification.

4.4.15 Special Requirements Regarding Key Compromise

Additionally, if a CIS Customer CA has discovered or has reason to believe its private key has been compromised, the CIS Customer is obligated to notify VeriSign as well as any Relying Parties.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

4.5.1.4 Events Recorded by CIS Customers (Type 1-2)

CIS Customers shall record in audit log files events relating to the security of the CA system such as:

- System start-up and shutdown,
- CA application start-up and shutdown,
- Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles),
- Changes to CA details and/or keys,
- Changes to Certificate creation policies e.g., validity period,
- Login and logoff attempts,
- Unauthorized attempts at network access to the CA system,
- Unauthorized attempts to access system files,
- Generation of a CA's own keys,
- Failed read and write operations on the Certificate and repository,
- Certificate lifecycle management-related events (e.g., approval or denial of Certificate Applications, issuance, revocation, and renewal), and
- Cryptographic module lifecycle management-related events (e.g., receipt, use, deinstallation, and retirement).

CIS Customers shall also collect and consolidate, either electronically or manually, security information not CA system generated such as:

- Key Generation Ceremony and key management databases,
- In the case of a key escrowing system, the back-up and recovery of end-user Subscriber private keys,
- Physical access logs,
- System configuration changes and maintenance,
- Personnel changes,
- Discrepancy and compromise reports,
- Records of the destruction of media containing key material, activation data, or personal Subscriber information, and
- Possession of activation data for CA private key operations.

4.8 Compromise and Disaster Recovery (Type 1-2)

CIS Customers shall maintain backups of their CA information within their Subdomains.

5. Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

5.1.1.5 CIS Customer Requirements (Type 1-2)

For CIS Customers, such requirements of physical security zones are defined in terms of layers instead of tiers. A layer is a set of barriers to physical intrusion or unauthorized access that requires mandatory access controls and a positive response for an individual to proceed to the next layer. Layers may share barriers provided such barriers are constructed of concrete or brick that is at least four inches thick and provide no other means of quick penetration other than the entrance door into the layer.

CIS Customers issuing Type 1 Certificates shall implement, at a minimum, two physical security layers, Layer 1 and Layer 2, with all cryptographic functions occurring at Layer 2.

CIS Customers issuing Type 2 Certificates shall implement, at a minimum, three physical security layers, Layers 1 through 3, with all cryptographic functions occurring at Layer 3.

5.1.2 Physical Access

5.1.2.4 Requirements for CIS Customers (Type 1-2)

CIS Customers shall control access to their CA or RA facilities. When installed and active, removable crypto modules shall be protected from equipment tampering and, when inactive, shall be placed in locked containers and stored in Layer 2 space or higher. All removable media and paper containing sensitive plain-text information shall be stored in secure containers. Additional requirements include:

- Minimizing exposure of privileged functions through definition of their function-specific roles or authorization groups,
- Access control enforcement of these roles or groups,
- Access controls to Layer 1 space shall not require individual identification. (Physical keys, combination locks or manned entry ways are sufficient.) Access controls to Layer 2 space shall contain a physical lock or cipher lock (e.g., a shared combination door lock). Access controls to Layer 3 space (Type 2 CAs) shall either provide electronic individual identification or require documentation in a manual access log before entry,
- The use of tamper resistant physical intrusion alarm systems to detect break-ins or unauthorized access to physical security layers within the facility, and

- Automated notification to outside alarm monitoring agency of a potential security breach when facility-based guards are not present.

Although not required, the use of biometric readers (e.g., hand geometry or iris scan) that provide two-factor authentication is recommended at Layer 3 space.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CIS Customer (Type 1-2)

Additionally, there are no specific stipulations for CIS Customers issuing only Type 1 Certificates. For Type 2 CIS Customer implementations, individuals may assume more than one role, but a given person may not assume both the CA system administrator and RA roles; and persons responsible for the audit logs that are removed from the CA system shall be different from the person(s) who command the CA signature key.

5.2.2 Number of Persons Required Per Task (Type 1-2)

Additionally, CIS Customers issuing Type 2 Certificates shall require a minimum of two persons filling trusted roles to perform the following tasks:

- Generating CA private keys;
- Backup of CA private keys;
- Activating and deactivating the CA's private key; or
- Renewal or re-key of CA certificate.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation (Type 1-2)

Additionally, CIS Customer CAs may pregenerate key pairs on behalf of Subscribers outside of hardware tokens when utilizing a key escrow system with security controls equivalent to Managed PKI Key Manager Software.

Generation of Subscriber key pairs is generally performed by functions contained within the Subscriber's browser software using the included software-based cryptographic module.

CIS Customer CA keys shall be generated in FIPS 140-1 Level 2 hardware. The each step of the key generation process shall be documented and the documentation signed by all persons involved in the ceremony. The persons involved shall be, at a minimum, a member of organizational IT management, a member of the computer operations staff, a member of the internal auditing function (or other witness that does not have direct influence over the PKI implementation), and a member of the staff that is

responsible for RA functions.

VeriSign-signed CIS Customer CA certificates shall be signed in a Key Generation Ceremony and shall conform to the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Security and Audit Requirements Guide.

6.1.2 Private Key Delivery to Entity (Type 1-2)

CIS Customer may use a non-VeriSign key escrow subsystem.

Where key pairs are pre-generated on CIS Customer CA systems, the entities distributing such key pairs shall take commercially reasonable efforts to provide physical security of the key pairs to prevent the loss, disclosure, modification, or unauthorized use of the private key(s) and ensure that the correct key pairs are received by the corresponding Subscriber.

6.1.9 Key Usage Purposes (As per X.509 v3 Key Usage Field) (Type 1-2)

Additional specifications for CIS Certificates are identified in Table 8.

		<i>VeriSign- signed CIS CAs</i>	<i>Type 1 End- User Subscribers</i>	<i>Type 2 End- User Subscribers (one key pair)</i>	<i>Type 2 Dual Key Pair Signature</i>	<i>Type 2 Dual Key Pair Encipherment</i>
Criticality		FALSE	FALSE	FALSE	FALSE	FALSE
0	<i>digitalSignature</i>	Clear	Set	Set	Set	Clear
1	<i>nonRepudiation</i>	Clear	Clear	Clear*	Clear*	Clear
2	<i>keyEncipherment</i>	Clear	Set	Set	Clear	Set
3	<i>dataEncipherment</i>	Clear	Clear	Clear	Clear	Clear
4	<i>keyAgreement</i>	Clear	Clear	Clear	Clear	Clear
5	<i>keyCertSign</i>	Set	Clear	Clear	Clear	Clear
6	<i>CRLSign</i>	Set	Clear	Clear	Clear	Clear
7	<i>encipherOnly</i>	Clear	Clear	Clear	Clear	Clear
8	<i>decipherOnly</i>	Clear	Clear	Clear	Clear	Clear

Table 8 – Settings for KeyUsage Extension

*The *nonRepudiation* bit is not required to be set in these Certificates because the PKI industry has not reached a consensus as to what the *nonRepudiation* bit means. Until such a consensus emerges, the *nonRepudiation* bit will not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not recognize the *nonRepudiation* bit. Therefore, setting the bit will not help Relying Parties make a trust decision. Consequently, the VTN CP requires that the *nonRepudiation* bit be cleared, although it may be set in the case of dual key pair signature Certificates not issued through a key escrow system.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Modules (Type 1-2)

CIS Customers shall perform all CA cryptographic operations on a cryptographic module rated at FIPS 140-1 level 2 or higher rating.

6.2.3 Private Key Escrow (Type 1-2)

CIS Customers using a key escrow system are permitted to escrow end-user Subscribers' encipherment private keys. Escrowed encipherment private keys shall be stored in encrypted form. Digital signature private keys of CAs or end-user Subscribers shall not be escrowed.

CIS Customer end-user Subscriber encipherment private keys shall only be recovered under the following circumstances:

- CIS Customers using a key escrow system shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's encipherment private key is, in fact, from the Subscriber and not an imposter,
- Such CIS Customers shall recover a Subscriber's encipherment private key without the Subscriber's request only for their legitimate business and lawful purposes, such as to comply with judicial or administrative process or a search warrant, to comply with business rules governing the recovery of corporate information, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such CIS Customers shall have personnel controls in place to prevent key escrow administrators and other persons from obtaining unauthorized access to private keys.

6.2.4 Private Key Backup (Type 1-2)

Additionally, Subscribers are permitted to backup their private keys given that they maintain unique control of the private key. It is highly recommended that Subscribers store backed up private keys in PKCS#12 or equivalent form.

6.2.7 Method of Activating Private Key

6.2.7.5 CIS Customer CA Private Keys (Type 1-2)

CIS Customer CA private keys shall be activated securely subject to the restrictions defined in CP § 5.2.2. Once the CA private key is activated, it may remain active until manually deactivated.

6.2.8 Method of Deactivating Private Key

6.2.8.4 CIS Customers (Type 1-2)

This section applies to a CIS Customer's own CAs. When an online CA is taken offline, the CIS Customer's personnel shall remove the token containing such CA's private key

from the reader in order to deactivate it. With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony (see CP § 6.1.1) in which such private keys are used for private key operations, the CIS Customer's personnel shall remove the token containing such CAs' private keys from the reader in order to deactivate them. Once removed from the reader, tokens shall be protected in accordance with CP § 5.1.2.

6.3.2 Usage Periods for the Public and Private Keys

Additionally, Table 9 defines the Operational Period for CIS Certificates.

Certificate Issued By:	Type 1	Type 2
VeriSign to CIS Customer offline CA NOTE: Customers are not required to use an offline CA, however where they do, the offline CA shall be hosted by VeriSign.	Up to 10 years	Up to 10 years
VeriSign to CIS Customer Issuing CA	Up to 7 years	Up to 7 years
CIS Customer CA to End-User Subscriber NOTE: encryption only End-User Subscriber certificates may be issued for 3 years	Up to 2 years	Up to 2 years

Table 9 – Certificate Operational Periods

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.4 Processing Centers and CIS Customers (Type 1-2)

CIS Customers shall generate activation data for their own CA private keys.

6.4.2 Activation Data Protection

6.4.2.3 CIS Customers (Type 1-2)

CIS Customers shall protect the activation data of their CA private key(s) against the loss, theft, modification or unauthorized disclosure of their activation data utilizing multiple trusted persons as defined in CP § 5.2.2. If activation data is written down, it shall be secured at the same level of protection as the associated private key and not be stored with the cryptographic module.

CIS Customers shall include in their disaster recovery plans provisions for providing activation data to multiple trusted persons in the event of a disaster at a disaster recovery site. CIS Customers shall maintain an audit trail of trusted persons having access to the activation data.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.4 Controls for CIS Customers (Type 1-2)

CIS Customers shall ensure that the systems maintaining CA software and RA information are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CP § 2.7.4. In addition, CIS Customers shall:

- Limit access to such systems to those individuals with a valid business reason for access. General application users shall not have accounts on the CA production servers,
- Logically separate access to such systems and information from other components. This separation prevents access except through defined processes,
- Use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information,
- Limit direct access to the CIS Customer's RA database maintaining Subscriber information to Trusted Persons and processes having a valid business reason for such access,
- Limit modification access to the CIS Customer's repository to Trusted Persons and processes having a valid business reason for such access,
- Require the use of passwords with a minimum character length of seven (7) and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and whenever necessary,
- Require identification and authentication for launching of CA services,
- Prohibit object re-use for CA random access memory and/or deleted files,
- Require use of cryptography for session communication and RA database access,
- Require archival of CA and end-user Subscriber history and audit data,
- Comply with audit criteria, and
- Validate a trusted path for identification of CA roles and associated identities.

6.5.2 Computer Security Rating (Type 1-2)

For CIS Customers, no stipulation.

6.6 Life Cycle Technical Controls (Type 1-2)

6.6.1 System Development Controls

6.6.1.3 CIS Customers (Type 2)

CIS Customers generating Type 2 Certificates shall implement the following system controls where appropriate:

- Use hardware and software that has been designed and developed in a controlled environment under a formal, documented development methodology (commercial-off-the-shelf applications already fall in this category),
- Purchase hardware and software to operate the CA in such a manner that reduces the risk that any particular component was tampered with and have it shipped and delivered to the CA location using controls that provide a continuous chain of accountability,
- No other applications, hardware devices, network connections, or component software shall be installed on the CA systems that do not support the CA operation,
- Only authorized software and applications shall be installed on the CA equipment in such a manner that prevents malicious code from intentionally or accidentally being installed. CA hardware and software shall be scanned for malicious code on first use and periodically thereafter, and
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined and secure manner.

6.6.2 Security Management Controls

6.6.2.3 Software Used by CIS Customers (Type 2)

Software for CA and RA functions designed to manage Type 2 Certificates shall be subject to checks to verify its integrity. CIS Customers shall have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at least once a day, CIS Customers shall validate the integrity of the CA system.

7. Certificate and CRL Profile

7.1 Certificate Profile

7.1.2.4 Basic Constraints

Additionally for CA Certificates issued to CIS Customers' for issuing End-User certificates, VeriSign shall set the "PathLenConstraint" field set to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.6 Certificate Policy Object Identifier

The object identifier for the applicable CIS CP Policy Identifier corresponding to each Type of Certificate is set forth in CP § 1.2. Processing Centers and CIS Customers shall populate the CertificatePolicies extension in each Certificate with the object identifier of the CP corresponding to the Certificate's Type set forth in CP § 1.2.

8. Specification Administration (Type 1-2)

8.3 CPS Approval Procedures

CIS Customers shall each have their own CPS. A CIS Customer's CPS will govern its Subdomain within the VTN. Entities wishing to become CIS Customers shall sign an agreement with VeriSign and work with VeriSign to modify the VeriSign CIS Customer CPS template to reflect the CIS Customer's CA environment. The modified CPS shall be submitted to the Practices and External Affairs Department of VeriSign. The Practices and External Affairs Department shall approve or reject the CPS or CPS modifications proposed by potential CIS Customers within its sole discretion. See **CP § 1.4.2 for the contact information for the Practices and External Affairs Department.**

9. Appendix

9.1 Acronyms and Definitions

Additional acronyms and definitions for terms not contained within the VTN CP glossary are specified here:

<i>Acronym</i>	<i>Term</i>
CIS	Certificate Interoperability Service
<i>Term</i>	<i>Definition</i>
Certificate Interoperability Service	A service offered by VeriSign or an Affiliate to allow an organization using a stand-alone Certificate server to become a CA within the VTN for purposes sending interoperable encrypted and/or digitally signed S/MIME (email) messages by having a VeriSign CA certify the organization's public key.
CIS Customer	An organization that has obtained CIS services from VeriSign or an Affiliate, whereby the organization becomes a CA within the VTN to issue Type 1 or Type 2 Certificates.
Encipherment	The process of using a cryptographic key and translation algorithm to translate clear text message into an encoded message that is only readable by translating the encoded message back into clear text using the corresponding cryptographic key. (a.k.a. encryption)
FIPS 140	Federal Information Processing Standards #140 which define the requirements for cryptographic modules. Level 1 describes software-based cryptographic modules (provided with Operating Systems such as Windows NT or higher). Level 2 describes requirements of entry level hardware based cryptographic modules (e.g., smart card or USB token)
Issuing CA	The CA that minted/generated the
Key Generation Process	Scaled back version of the VeriSign Key Generation Ceremony used by CIS Customers when generating their CA keys. This process

Acronym	Term
	must be witnessed by persons as defined in § 6.1.1
Layer	A security zone as defined in § 5.1.1.5
RFC 822	IETF standard (Request for Comment) #822 which defines the format of Internet email addresses (e.g., recipientAlias@company.com). Details can be located at www.ietf.org/rfc/rfc822.txt
Type of certificate	A specified level of assurances associated with a Certificate as defined within this CP. See CP § 1.1.1.

9.2 Section Number Cross Reference

The VTN CP section numbers are listed in the following table. A status of “*Modified*” indicates that this CIS CP Supplement has modified language pertaining to CIS Customers. A status of “*New*” indicates that the associated section does not exist in the VTN CP and was created specifically for CIS Customers. A status of “*Unmodified*” indicates that the VTN CP language is sufficient for CIS Customers.

Section #	Title	Status
	Modified Sections	
1.	Introduction	Modified
1.1	Overview	Modified
1.1.1	Policy Overview	Modified
1.2	Identification	Modified
1.4.3	Person Determining CPS Suitability for the Policy	Modified
2.1.5	Repository Obligations	Modified
2.2.1.3	Certification Authority Limitations of Liability	Modified
2.2.3.1	Subscriber Warranties	Modified
2.3.3	Administrative Processes	Modified
2.5	Fees	Modified
2.7.1	Frequency of Entity Compliance Audit	Modified
2.7.2	Identity/ Qualifications of Auditor	Modified
3.1.1	Types of Names	Modified
3.1.4	Uniqueness of Names	Modified
3.1.8.2	Authentication of the Identity of CAs and RAs	Modified
3.1.9	Authentication of Individual Identity	Modified
3.1.9.2.1	Class 2 Managed PKI Certificates	Modified
3.2	Routine Rekey (Renewal)	Modified
4.1.1	Certificate Applications for End-User Subscriber Certificates	Modified
4.4.9	CRL Issuance Frequency (If Applicable)	Modified
4.4.15	Special Requirements Regarding Key Compromise	Modified
4.8	Compromise and Disaster Recovery	Modified
5.2.1.1	Gateway Customer and Processing Center Trusted Roles	Modified
5.2.2	Number of Persons Required Per Task	Modified
6.1.1	Key Pair Generation	Modified

Section #	Title	Status
6.1.2	Private Key Delivery to Entity	Modified
6.1.9	Key Usage Purposes (As per X.509 v3 Key Usage Field)	Modified
6.2.1	Standards for Cryptographic Modules	Modified
6.2.3	Private Key Escrow	Modified
6.2.4	Private Key Backup	Modified
6.3.2	Usage Periods for the Public and Private Keys	Modified
6.4.1.4	Processing Centers and CIS Customers (Type 1-2)	Modified
6.5.2	Computer Security Rating	Modified
7.1.2.4	Basic Constraints	Modified
7.1.6	Certificate Policy Object Identifier	Modified
8.3	CPS Approval Procedures	Modified
Appendix	Table of Acronyms	Modified
Appendix	Definitions	Modified
Newly Authored Sections		
1.3.4.1.4	CIS Type 1-2 Certificates	New
2.7.4.5	Audit of CIS Customer (Type 1-2)	New
4.5.1.4	Events Recorded by CIS Customers (Type 1-2)	New
5.1.1.5	CIS Customer Requirements (Type 1-2)	New
5.1.2.4	Requirements for CIS Customers (Type 1-2)	New
6.2.7.5	CIS Customer CA Private Keys (Type 1-2)	New
6.2.8.4	CIS Customers (Type 1-2)	New
6.4.2.3	CIS Customers (Type 1-2)	New
6.5.1.4	Controls for CIS Customers (Type 1-2)	New
6.6.1.3	CIS Customers (Type 2)	New
6.6.2.3	Software Used by CIS Customers (Type 2)	New
Unmodified Sections		
1.1.2	VTN Suite of Services	Unmodified
1.1.2.1	Certificate Distribution Services	Unmodified
1.1.2.1.1	VeriSign Managed PKI ®	Unmodified
1.1.2.1.2	VeriSign Affiliate Program	Unmodified
1.1.2.1.3	Universal Service Center Program and Other Reseller Programs	Unmodified
1.1.2.1.4	The Web Host Program	Unmodified
1.1.2.1.5	VeriSign Gateway Services	Unmodified
1.1.2.2	Value-Added Certification Services	Unmodified
1.1.2.2.1	Authentication Services	Unmodified
1.1.2.2.2	VeriSign Digital Notarization Service	Unmodified
1.1.2.2.3	NetSure SM Protection Plan	Unmodified
1.1.2.3	Special Certificate Types	Unmodified
1.1.2.3.1	Wireless Certificate Services	Unmodified
1.1.2.3.2	VeriSign Managed PKI Key Manager Services	Unmodified
1.1.2.3.3	VeriSign Roaming Service	Unmodified
1.3	Community and Applicability	Unmodified

Section #	Title	Status
1.3.1	Certification Authorities	Unmodified
1.3.2	Registration Authorities	Unmodified
1.3.3	End Entities	Unmodified
1.3.4	Applicability	Unmodified
1.3.4.1	Suitable Applications	Unmodified
1.3.4.1.1	Class 1 Certificates	Unmodified
1.3.4.1.2	Class 2 Certificates	Unmodified
1.3.4.1.3	Class 3 Certificates	Unmodified
1.3.4.1.3.1	Class 3 Individual Certificates	Unmodified
1.3.4.1.3.2	Class 3 Organizational Certificates	Unmodified
1.3.4.2	Restricted Applications	Unmodified
1.3.4.3	Prohibited Applications	Unmodified
1.4	Contact Details	Unmodified
1.4.1	Specification Administration Organization	Unmodified
1.4.2	Contact Person	Unmodified
2.	General Provisions	Unmodified
2.1	Obligations	Unmodified
2.1.1	CA Obligations	Unmodified
2.1.2	RA Obligations	Unmodified
2.1.3	Subscriber Obligations	Unmodified
2.1.4	Relying Party Obligations	Unmodified
2.2	Liability	Unmodified
2.2.1	Certification Authority Liability	Unmodified
2.2.1.1	Certification Authority Warranties to Subscribers and Relying Parties	Unmodified
2.2.1.2	Certification Authority Disclaimers of Warranties	Unmodified
2.2.1.4	Force Majeure	Unmodified
2.2.2	Registration Authority Liability	Unmodified
2.2.3	Subscriber Liability	Unmodified
2.2.3.2	Private Key Compromise	Unmodified
2.2.4	Relying Party Liability	Unmodified
2.3	Financial Responsibility	Unmodified
2.3.1	Indemnification by Subscribers and Relying Parties	Unmodified
2.3.1.1	Indemnification by Subscribers	Unmodified
2.3.1.2	Indemnification by Relying Parties	Unmodified
2.3.2	Fiduciary Relationships	Unmodified
2.4	Interpretation and Enforcement	Unmodified
2.4.1	Governing Law	Unmodified
2.4.2	Severability, Survival, Merger, Notice	Unmodified
2.4.3	Dispute Resolution Procedures	Unmodified
2.4.3.1	Disputes Among VeriSign, Affiliates, and Customers	Unmodified
2.4.3.2	Disputes with End-User Subscribers or Relying Parties	Unmodified
2.5.1	Certificate Issuance or Renewal Fees	Unmodified
2.5.2	Certificate Access Fees	Unmodified

Section #	Title	Status
2.5.3	Revocation or Status Information Access Fees	Unmodified
2.5.4	Fees for Other Services Such as Policy Information	Unmodified
2.5.5	Refund Policy	Unmodified
2.6	Publication and Repository	Unmodified
2.6.1	Publication of CA Information	Unmodified
2.6.1.1	Publication by VeriSign and Affiliates	Unmodified
2.6.1.2	Publication by Gateway Customers	Unmodified
2.6.2	Frequency of Publication	Unmodified
2.6.3	Access Controls	Unmodified
2.6.4	Repositories	Unmodified
2.7	Compliance Audit	Unmodified
2.7.2.1	Personnel Performing Self-Audits	Unmodified
2.7.2.2	Qualifications of Third-Party Audit Firms	Unmodified
2.7.3	Auditor's Relationship to Audited Party	Unmodified
2.7.4	Topics Covered by Audit	Unmodified
2.7.4.1	Self-Audits of Gateway Customers	Unmodified
2.7.4.2	Self-Audits of Managed PKI Customers	Unmodified
2.7.4.3	Audit of an Managed PKI Customer	Unmodified
2.7.4.4	Audit of VeriSign or an Affiliate	Unmodified
2.7.5	Actions Taken as a Result of Deficiency	Unmodified
2.7.6	Communications of Results	Unmodified
2.8	Confidentiality and Privacy	Unmodified
2.8.1	Types of Information to be Kept Confidential and Private	Unmodified
2.8.2	Types of Information Not Considered Confidential or Private	Unmodified
2.8.3	Disclosure of Certificate Revocation/Suspension Information	Unmodified
2.8.4	Release to Law Enforcement Officials	Unmodified
2.8.5	Release as Part of Civil Discovery	Unmodified
2.8.6	Disclosure Upon Owner's Request	Unmodified
2.8.7	Other Information Release Circumstances	Unmodified
2.9	Intellectual Property Rights	Unmodified
2.9.1	Property Rights in Certificates and Revocation Information	Unmodified
2.9.2	Property Rights in the CP	Unmodified
2.9.3	Property Rights in Names	Unmodified
2.9.4	Property Rights in Keys and Key Material	Unmodified
3.	Identification and Authentication	Unmodified
3.1	Initial Registration	Unmodified
3.1.2	Need for Names to be Meaningful	Unmodified
3.1.3	Rules for Interpreting Various Name Forms	Unmodified
3.1.5	Name Claim Dispute Resolution Procedure	Unmodified
3.1.6	Recognition, Authentication, and Role of Trademarks	Unmodified
3.1.7	Method to Prove Possession of Private Key	Unmodified
3.1.8	Authentication of Organization Identity	Unmodified
3.1.8.1	Authentication of the Identity of Organizational End-User Subscribers	Unmodified

Section #	Title	Status
3.1.8.1.1	Authentication for Retail Organizational Certificates	Unmodified
3.1.8.1.2	Authentication for Managed PKI for SSL or Managed PKI for SSL Premium Edition	Unmodified
3.1.8.1.3	Authentication for Class 3 Organizational ASB Certificates	Unmodified
3.1.9.1	Class 1 Certificates	Unmodified
3.1.9.2	Class 2 Certificates	Unmodified
3.1.9.2.2	Class 2 Retail Certificates	Unmodified
3.1.9.3	Class 3 Individual Certificates	Unmodified
3.2.1	Renewal of End-User Subscriber Certificates	Unmodified
3.2.2	Renewal of CA Certificates	Unmodified
3.3	Rekey After Revocation	Unmodified
3.4	Revocation Request	Unmodified
4.	Operational Requirements	Unmodified
4.1	Certificate Application	Unmodified
4.1.2	Certificate Applications for CA or RA Certificates	Unmodified
4.2	Certificate Issuance	Unmodified
4.2.1	Issuance of End-User Subscriber Certificates	Unmodified
4.2.2	Issuance of CA and RA Certificates	Unmodified
4.3	Certificate Acceptance	Unmodified
4.4	Certificate Suspension and Revocation	Unmodified
4.4.1	Circumstances for Revocation	Unmodified
4.4.1.1	Circumstances for Revoking End-User Subscriber Certificates	Unmodified
4.4.1.2	Circumstances for Revoking CA or RA Certificates	Unmodified
4.4.2	Who Can Request Revocation	Unmodified
4.4.2.1	Who Can Request Revocation of an End-User Subscriber Certificate	Unmodified
4.4.2.2	Who Can Request Revocation of a CA or RA Certificate	Unmodified
4.4.3	Procedure for Revocation Request	Unmodified
4.4.3.1	Procedure for Requesting the Revocation of an End-User Subscriber Certificate	Unmodified
4.4.3.2	Procedure for Requesting the Request Revocation of a CA or RA Certificate	Unmodified
4.4.4	Revocation Request Grace Period	Unmodified
4.4.5	Circumstances for Suspension	Unmodified
4.4.6	Who Can Request Suspension	Unmodified
4.4.7	Procedure for Suspension Request	Unmodified
4.4.8	Limits on Suspension Period	Unmodified
4.4.10	Certificate Revocation List Checking Requirements	Unmodified
4.4.11	On-Line Revocation/Status Checking Availability	Unmodified
4.4.12	On-Line Revocation Checking Requirements	Unmodified
4.4.13	Other Forms of Revocation Advertisements Available	Unmodified
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements	Unmodified

Section #	Title	Status
4.5	Security Audit Procedures	Unmodified
4.5.1	Types of Events Recorded	Unmodified
4.5.1.1	Events Recorded by Processing Centers	Unmodified
4.5.1.2	Events Recorded by Service Centers, Managed PKI Customers	Unmodified
4.5.1.3	Events Recorded by Gateway Customers	Unmodified
4.5.2	Frequency of Processing Log	Unmodified
4.5.3	Retention Period for Audit Log	Unmodified
4.5.4	Protection of Audit Log	Unmodified
4.5.5	Audit Log Backup Procedures	Unmodified
4.5.6	Audit Collection System	Unmodified
4.5.7	Notification to Event-Causing Subject	Unmodified
4.5.8	Vulnerability Assessments	Unmodified
4.6	Records Archival	Unmodified
4.6.1	Types of Events Recorded	Unmodified
4.6.2	Retention Period for Archive	Unmodified
4.6.3	Protection of Archive	Unmodified
4.6.4	Archive Backup Procedures	Unmodified
4.6.5	Requirements for Time-Stamping of Records	Unmodified
4.6.6	Archive Collection System	Unmodified
4.6.7	Procedures to Obtain and Verify Archive Information	Unmodified
4.7	Key Changeover (Renewal)	Unmodified
4.8.1	Computing Resources, Software, and/or Data Are Corrupted	Unmodified
4.8.2	Entity Public Key is Revoked	Unmodified
4.8.3	Entity Key is Compromised	Unmodified
4.8.4	Secure Facility After a Natural or Other Type of Disaster	Unmodified
4.9	CA Termination	Unmodified
5.	Physical, Procedural, and Personnel Security Controls	Unmodified
5.1	Physical Controls	Unmodified
5.1.1	Site Location and Construction	Unmodified
5.1.1.1	Gateway Customer Requirements	Unmodified
5.1.1.2	Managed PKI Customer Requirements	Unmodified
5.1.1.3	Service Center Requirements	Unmodified
5.1.1.4	Processing Center Requirements	Unmodified
5.1.2	Physical Access	Unmodified
5.1.2.1	Requirements for Gateway Customers and Managed PKI Customers	Unmodified
5.1.2.2	Service Center Requirements	Unmodified
5.1.2.3	Processing Center Requirements	Unmodified
5.1.3	Power and Air Conditioning	Unmodified
5.1.4	Water Exposures	Unmodified
5.1.5	Fire Prevention and Protection	Unmodified
5.1.6	Media Storage	Unmodified

Section #	Title	Status
5.1.7	Waste Disposal	Unmodified
5.1.8	Off-Site Backup	Unmodified
5.2	Procedural Controls	Unmodified
5.2.1	Trusted Roles	Unmodified
5.2.1.2	Service Center and Managed PKI Customer Trusted Roles	Unmodified
5.2.1.3	ASB Customer Trusted Roles	Unmodified
5.2.3	Identification and Authentication for Each Role	Unmodified
5.3	Personnel Controls	Unmodified
5.3.1	Background, Qualifications, Experience, and Clearance Requirements	Unmodified
5.3.2	Background Check Procedures	Unmodified
5.3.2.1	Background Check Procedures for Gateway Customers, ASB Customers, and Managed PKI Customers	Unmodified
5.3.2.2	Background Check Procedures for Service Centers and Processing Centers	Unmodified
5.3.3	Training Requirements	Unmodified
5.3.4	Retraining Frequency and Requirements	Unmodified
5.3.5	Job Rotation Frequency and Sequence	Unmodified
5.3.6	Sanctions for Unauthorized Actions	Unmodified
5.3.7	Contracting Personnel Requirements	Unmodified
5.3.8	Documentation Supplied to Personnel	Unmodified
6.	Technical Security Controls	Unmodified
6.1	Key Pair Generation and Installation	Unmodified
6.1.3	Public Key Delivery to Certificate Issuer	Unmodified
6.1.4	CA Public Key Delivery to Users	Unmodified
6.1.5	Key Sizes	Unmodified
6.1.6	Public Key Parameters Generation	Unmodified
6.1.7	Parameter Quality Checking	Unmodified
6.1.8	Hardware/Software Key Generation	Unmodified
6.2	Private Key Protection	Unmodified
6.2.2	Private Key (m out of n) Multi-Person Control	Unmodified
6.2.5	Private Key Archival	Unmodified
6.2.6	Private Key Entry into Cryptographic Module	Unmodified
6.2.7	Method of Activating Private Key	Unmodified
6.2.7.1	End-User Subscriber Private Keys	Unmodified
6.2.7.1.1	Class 1 Certificates	Unmodified
6.2.7.1.2	Class 2 Certificates	Unmodified
6.2.7.1.3	Class 3 Certificates Other Than Administrator Certificates	Unmodified
6.2.7.2	Administrators' Private Keys	Unmodified
6.2.7.2.1	Administrators	Unmodified
6.2.7.2.2	Managed PKI Administrators using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)	Unmodified
6.2.7.3	Gateway Customers' Private Keys	Unmodified

Section #	Title	Status
6.2.7.4	Private Keys Held by Processing Centers	Unmodified
6.2.8	Method of Deactivating Private Key	Unmodified
6.2.8.1	End-User Subscribers	Unmodified
6.2.8.1.1	Class 1 Certificates	Unmodified
6.2.8.1.2	Class 2 Certificates	Unmodified
6.2.8.1.3	Class 3 Certificates	Unmodified
6.2.8.2	Gateway Customers	Unmodified
6.2.8.3	Processing Centers	Unmodified
6.2.9	Method of Destroying Private Key	Unmodified
6.2.9.1	Gateway Customers	Unmodified
6.2.9.2	Processing Centers	Unmodified
6.3	Other Aspects of Key Pair Management	Unmodified
6.3.1	Public Key Archival	Unmodified
6.4	Activation Data	Unmodified
6.4.1	Activation Data Generation and Installation	Unmodified
6.4.1.1	End-User Subscribers	Unmodified
6.4.1.2	Administrators	Unmodified
6.4.1.3	Gateway Customers	Unmodified
6.4.2	Activation Data Protection	Unmodified
6.4.2.1	End-User Subscribers and Gateway Customers (Class 1)	Unmodified
6.4.2.2	Processing Centers	Unmodified
6.4.3	Other Aspects of Activation Data	Unmodified
6.4.3.1	Activation Data Transmission	Unmodified
6.4.3.2	Activation Data Destruction	Unmodified
6.5	Computer Security Controls	Unmodified
6.5.1	Specific Computer Security Technical Requirements	Unmodified
6.5.1.1	Controls for Processing Centers	Unmodified
6.5.1.2	Controls for Gateway Customers	Unmodified
6.5.1.3	Controls for Service Centers and Managed PKI Customers	Unmodified
6.6	Life Cycle Technical Controls	Unmodified
6.6.1	System Development Controls	Unmodified
6.6.1.1	Software Used by Gateway Customers	Unmodified
6.6.1.2	Software Used by Managed PKI Customers, Service Centers, and Processing Centers	Unmodified
6.6.2	Security Management Controls	Unmodified
6.6.2.1	Software Used by Gateway Class 1 Customers	Unmodified
6.6.2.2	Software Used by Managed PKI Customers, Service Centers, and Processing Centers	Unmodified
6.6.3	Life Cycle Security Ratings	Unmodified
6.7	Network Security Controls	Unmodified
6.8	Cryptographic Module Engineering Controls	Unmodified
7.	Certificate and CRL Profile	Unmodified
7.1	Certificate Profile	Unmodified
7.1.1	Version Number(s)	Unmodified

Section #	Title	Status
7.1.2	Certificate Extensions	Unmodified
7.1.2.1	Key Usage	Unmodified
7.1.2.2	Certificate Policies Extension	Unmodified
7.1.2.3	Subject Alternative Names	Unmodified
7.1.2.5	Extended Key Usage	Unmodified
7.1.2.6	CRL Distribution Points	Unmodified
7.1.2.7	Authority Key Identifier	Unmodified
7.1.2.8	Subject Key Identifier	Unmodified
7.1.3	Algorithm Object Identifiers	Unmodified
7.1.4	Name Forms	Unmodified
7.1.5	Name Constraints	Unmodified
7.1.7	Usage of Policy Constraints Extension	Unmodified
7.1.8	Policy Qualifiers Syntax and Semantics	Unmodified
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	Unmodified
7.2	CRL Profile	Unmodified
7.2.1	Version Number(s)	Unmodified
7.2.2	CRL and CRL Entry Extensions	Unmodified
8.	Specification Administration	Unmodified
8.1	Specification Change Procedures	Unmodified
8.1.1	Items that Can Change Without Notification	Unmodified
8.1.2	Items that Can Change with Notification	Unmodified
8.1.2.1	List of Items	Unmodified
8.1.2.2	Notification Mechanism	Unmodified
8.1.2.3	Comment Period	Unmodified
8.1.2.4	Mechanism to Handle Comments	Unmodified
8.1.3	Changes Requiring Changes in the Certificate Policy OID or CPS Pointer	Unmodified
8.2	Publication and Notification Policies	Unmodified
8.2.1	Items Not Published in the CP	Unmodified
8.2.2	Distribution of the CP	Unmodified

* * * End of Document * * *